

LOUSY DISINFORMATION SCHEME

BY **CHRISTOPHER SALGADO,**

CEO OF ALL POINTS INVESTIGATIONS, LLC

It's the holiday season! Eggnog, lights, songs, worship, family, memory-inspiring times and yes, presents! At least for the little ones, I suppose. Nonetheless, you've arrived at yet another season of fun – with a sprinkle of chaos, I'm sure.

While you and your family are locked on target to have fun at grandma's, you carve out an opportunity to catch up on an overdue OSINT and cyber case. Alas, the modernization of conversations between people not only occur around the fireplace around this time but also all over the internet. Stories of the good, the bad and the ugly perpetually circulate throughout social media platforms, video channels, online photo albums, podcasts and others. While some stories are weaved to promote happiness and smiles across the faces of

connected loved ones, others are deviously manufactured inside the darkened depths of the minds of bad actors. These latter stories are maliciously designed to stand up welcoming but fraudulent attribution for bad actors or their illicit campaigns – known as cover stories.

Given the above setting, the task of ingesting information on your subject can very well become quite the task not due to a lack of information but due to an abundance of information. This is because misinformation spreads like wildfire. Discerning fact from fiction can sometimes challenge even the most astute investigator. The fiction that I am referencing is defined as misinformation and disinformation. Similar sounds but very different values within an investigative analysis. Misinformation highlights intentionally spreading inaccurate information while disinformation is the result of intentionally crafted deception aimed to manipulate. Both can be nicely gift-wrapped and appear legitimate. AI-generated or manually generated video may successfully sell its story to sound minds. So how do these fireplace stories spread?

Some physical holiday gatherings have nearly been replaced with digital platform gatherings. The change is folks now share stories in online forums or social media threads versus at family dinner tables. This evolved setting stokes the fire for a breeding ground for disinformation. After all, social media posts travel across X, TikTok and Instagram faster than Santa destined to beat last year's worldwide travel record.

Additionally, AI-generated content, such as deepfakes and synthetic voices can create effective disinformation resulting in false statements, articles, photos or videos. Even old school, ineffective shams can be overhauled and primed for an audience keen on the old scam but not the upgraded version of Scam 2.0.

So how do you defeat this? The challenges for investigators are multi-faceted.

First, you must defend yourself from information overload and verification overload. This entails sifting through a plethora – sometimes



thousands – of posts, images, text, etc. A considerable amount of time can fall victim to this step. I'm certain we're all too familiar with this.

Second, you've got the danger resulting from the speed of how fast content travels and is viewed by people and companies. By the time truth on the matter surfaces, the molded fiction may have caused irreversible damage in the court of public opinion.

Third, evidentiary concerns must be considered. More and more courts are routinely demanding online evidence showcase verifiable metadata. While these mandates are excellent quality assurance across the industry, you must be familiar with that sort of scientific extraction process: measurable and repeatable. Information must be validated by reliable sources. It does no one any good if you just recycle misinformation or disinformation as your citations. On the contrary, it raises the impact of the damage.

December especially can be a Petri dish for scams that exploit goodwill through sham charities, fake e-cards delivering malware and phishing schemes disguised as delivery notices. Unfortunately, the chapter on December/holiday scams enjoys a much lengthier list of examples than that.

Some best practices and tools to help thwart these white elephant gifts are to:

1. Examine every piece of data before relying on it; if your case isn't intended to go to court, manage it as if it will. Stand up the most rigorous pseudo firewalls that support your findings.
2. Identify and capture original information, complete with timestamps and other metadata.
3. Cross-check your evidence with other known – and reliable – sources. (We can't always use Wikipedia.)
4. Install an effective video and photo analysis to help detect any nefarious manipulation of such media.
5. Set up expectations with your client on what's out there and what can be ascertained. Just because a thought exists in the WWW, it doesn't make it gospel.

Note that there are several more processes that can be instituted into a rigorous verification checkpoint to ensure that you safeguard integrity throughout your investigations. We all know, it's best to deliver facts versus more stories. If your client can't appreciate that and they gravitate towards the latest and shiniest of online gossip, maybe it's best that you grab a cup of eggnog and sit this one out. Invoices come and go but your reputation stays with you – good or bad.

I wish I could say it's going to get better but, alas, my magical eight ball proclaims DON'T COUNT ON IT. Information has long become the oil of the digital age. The effective arms race has transitioned from a race to weapons to a race for more and more information. *Seinfeld's* Newman said it best: "When you control the mail, you control... information." Yes, he was a mailman referencing mail but his inferred thought was that information is power. His comical declaration fiercely rings true today. However, aggravating this scenario is,

there are large amounts of falsehoods intentionally or unintentionally embedded inside our otherwise World Wide Web of truth. Given the pace of bad data, this problem will only intensify and likely intensify aggressively. AI-generated disinformation is becoming harder to spot. Users of the internet – basically everyone – are becoming more and more skeptical of online information. By default, your mission could become more difficult whether the destination of your report is a corporate office, a courthouse, administration panel or the desk of law enforcement. It is critical for investigators to continue evolving by learning the latest and greatest tools and methods to negate the problem of inheriting bad data into your assessment.

As holidays prepare to create new memories by welcoming our happiness and less defensive statuses, we must remind ourselves that, in the cyber and OSINT world, false narratives can divide, deceive and harm. This is true in our professional and personal lives.

The role for investigators should be clear: shine a big holiday beacon into the digital darkness, unwrap the deceitful packaging and restore clarity and confidence in your data. At that point, we can all take a big swig of eggnog – or hot ham water, whatever floats your boat – and ease back into our rocking chairs as we sigh from relief, highlighting our victorious impact during a holiday season that avoided morphing a visit with that joyous Santa into the unwelcomed Krampus! **PI**



Christopher Salgado is the CEO of All Points Investigations, LLC, a global cyber and physical investigative firm serving Fortune-listed corporations, law firms, and other entities. A former Facebook investigator, he brings over 20 years of expertise in cyber investigations, OSINT, cryptocurrency, social engineering, and threat management. His work spans corporate risk, brand protection, cults, cyberstalkers, SIU matters and others. In 2024, he was named a Top Investigator by

PI Magazine. Christopher is a member of the London Speaker Bureau and a keynote speaker at industry events, including CrimeCon. He has briefed agencies such as the FBI, DEA, HSI, CBP, Interpol, Europol and members of the EU Commission. He is also the Founder of Anti-Hackathon, an online safety initiative, and AGGOSO™ Training, an advanced OSINT education program. He may be reached at csalgado@allpointsinv.com

- Asset & Witness Locates
- Market Sweeps
- CnD Service
- Criminal
- Seizures
- Death
- Fraud
- Civil

ALL POINTS INVESTIGATIONS, LLC
A GLOBAL INVESTIGATIONS FIRM
Former Facebook Investigator
Social Media Investigations
Cyber Investigations
Surface web • Deep web • Dark web

- Hazard Risk & Vulnerability Assessments
- Travel / Event / Property Risk Assessments
- Business Resiliency Assessments
- Competitor Intelligence
- Litigation Support
- Digital Forensics
- Social Media

Cyber Consulting!

www.AllPointsInv.com | info@allpointsinv.com | 408-365-4144 | Florida Agency License A1800260
Surveillance | Supply Chain | Corporate Security | Online & Brand Protection